Toegangslezers

Configuratiehandleiding

2N TELEKOMUNIKACE a.s.
Modřanská 621 | Prague 4 | 143 01

2N.com

Inhoudsopgave

Eerste aanmelding

Apparaten op het netwerk vinden

Om toegang te krijgen tot de interface, moet u het IP-adres van het apparaat of de domeinnaam van het apparaat kennen. Het apparaat moet verbonden zijn met het lokale IP-netwerk en moet van stroom worden voorzien.

Domeinnaam

Om toegang te krijgen tot de webconfiguratie-interface, kunt u een domeinnaam in de browser invoeren in het formaat “hostname.local” in plaats van het IP-adres. De hostnaam van een nieuw apparaat bestaat uit de productnaam en het serienummer van het apparaat. Gebruik bij het invoeren van een hostnaam alleen letters en cijfers; gebruik geen spaties, punten, streepjes of andere speciale tekens.

Standaarddomeinnaam van het apparaat : 2NAccessUnit-{serienummer zonder streepjes}.local (bijvoorbeeld: “2NAccessUnit-0000000001.local”)

Het formaat van de naam van het specifieke apparaat wordt gespecificeerd in de Installatiehandleiding van het product in het hoofdstuk Domeinnaam.

TIP
U kunt de hostnaam later wijzigen in de webconfiguratie-interface op **Systeem > Netwerkverbinding > tabblad Geavanceerde configuratie > Hostnaam**.

Aanmelden met een domeinnaam biedt voordelen bij het gebruik van een dynamisch IP-adres van een apparaat. Terwijl het dynamische IP-adres verandert, blijft het domeinnaam hetzelfde. Voor het domeinnaam is het mogelijk om certificaten te genereren die zijn ondertekend door een vertrouwde certificeringsinstantie.

IP-adres van het apparaat

Standaard gebruikt het apparaat een dynamisch IP-adres dat door de DHCP-server wordt toegewezen.

Om het IP-adres van een 2N-apparaat op uw lokale netwerk te achterhalen, gebruikt u de 2N IP Utility. De toepassing 2N IP Utility kan worden gedownload van de website 2N.com. Voor de installatie moet Microsoft .NET Framework 4.7.2 geïnstalleerd zijn.

Afhankelijk van de mogelijkheden van het apparaat kunt u het IP-adres ook op een van de volgende manieren achterhalen:

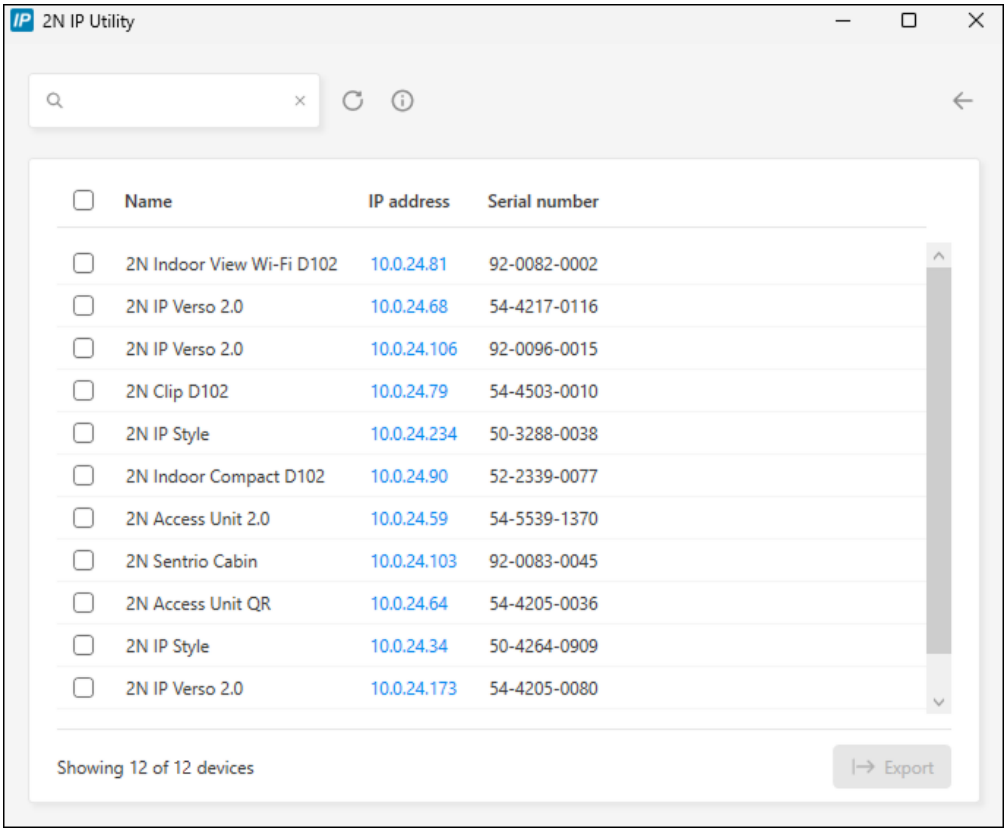
- met de RESET knop

Een IP-adres krijgen met 2N IP Utility

Om het IP-adres van een 2N-apparaat op uw lokale netwerk te achterhalen, gebruikt u de 2N IP Utility. De toepassing 2N IP Utility kan worden gedownload van de website 2N.com. Voor de installatie moet Microsoft .NET Framework 4.7.2 geïnstalleerd zijn.

1. Start het installatieprogramma 2N IP Utility.
2. De installatiewizard leidt u door de installatie.

3. Nadat u de toepassing 2N IP Utility hebt geïnstalleerd, start u de toepassing in het menu Start van het Microsoft Windows-besturingssysteem.
   Na het starten begint de toepassing automatisch het lokale netwerk af te zoeken naar alle 2N- en AXIS-apparaten die een IP-adres toegewezen hebben gekregen of statisch ingesteld zijn via DHCP. Deze apparaten worden vervolgens in de tabel weergegeven.



4. Selecteer het apparaat dat u wilt configureren uit de lijst en klik er met de linkermuisknop op. Hierdoor wordt de rechterkant van het webconfiguratiescherm geopend.

TIP

- De webconfiguratie-interface is ook toegankelijk via de knop **Open in external browser**, waarmee u de interface in een apart browservenster kunt openen.
- Klik op een apparaat in de lijst om gedetailleerde informatie te bekijken. Klik op de knop **IP settings** om het IP-adres te wijzigen door het gewenste statische IP-adres in te voeren of door DHCP te activeren.
- Met de applicatie kunt u ook geselecteerde apparaten exporteren naar een CSV-bestand. Selecteer eerst het apparaat door de vakjes voor elk apparaat in de lijst aan te vinken en gebruik dan de knop **Export** die onderaan het venster verschijnt. Het geëxporteerde bestand bevat de naam, het IP-adres en het serienummer van de geselecteerde apparaten.

De standaardreferenties zijn:
Gebruikersnaam: **Admin**
Wachtwoord: **2n**
Na de eerste keer inloggen dient u direct uw wachtwoord te wijzigen.

TIP
Het wordt aanbevolen om een wachtwoord te gebruiken dat moeilijk te kraken is. Het wordt afgeraden om namen, plaatsnamen of namen van voorwerpen in wachtwoorden te gebruiken, met name als deze een directe link hebben met de gebruiker.

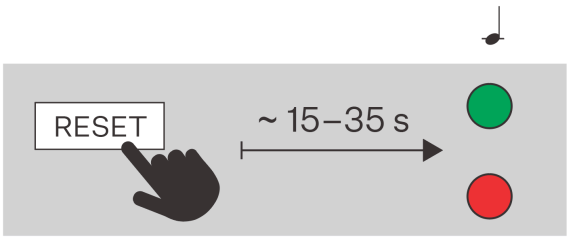
Voor een hogere wachtwoordbeveiliging raden wij aan:

- gebruik maken van een willekeurige wachtwoordgenerator
- een wachtwoordlengte van minimaal 12 tekens
- een combinatie van verschillende tekens uit verschillende tekensets (bijvoorbeeld kleine/hoofdletters, cijfers, speciale tekens, enzovoort)

Het achterhalen van het IP-adres met behulp van hardware

Volg de onderstaande stappen om uw huidige IP-adres te achterhalen:

1. Houd de RESET-knop ingedrukt.
   a. Wacht tot de rode en groene LEDs op het apparaat gelijktijdig oplichten en het geluidsalarm afgaat (ongeveer 15-35 seconden).
2. Laat de RESET-knop los.
3. Het apparaat zal automatisch de huidige IP-adres via spraak doorgeven.



OPMERKING
De tijd tussen het indrukken van de RESET-knop en de eerste licht- en geluidssignalering ligt tussen 15 en 35 seconden, afhankelijk van het specifieke model van het apparaat.

DHCP schakelen

Standaard gebruikt het apparaat een dynamisch IP-adres dat door de DHCP-server wordt toegewezen.

Dynamisch IP-adres

DHCP (Dynamic Host Configuration Protocol) is een netwerkprotocol dat een lijst met beschikbare IP-adressen bijhoudt en deze automatisch toewijst aan apparaten op het lokale netwerk. Het toegewezen IP-adres is dynamisch, dus het apparaat kan na een bepaalde tijd (leasetijd) een nieuw IP-adres toegewezen krijgen.

Statisch IP-adres

Als het IP-adres van het apparaat ongewijzigd moet blijven, moet u de toewijzing van IP-adressen door de DHCP-server op het apparaat uitschakelen. U kunt de DHCP-server uitschakelen in de webconfiguratie-interface of via de hardware op het apparaat.

OPMERKING
De specifieke waarden voor het statische IP-adres kunnen alleen worden ingesteld in de webconfiguratie-interface van het apparaat.

Netwerkparameters instellen in de webconfiguratie-interface

1. Ga naar de webconfiguratie-interface.
2. Ga naar **Systeem > Netwerkverbinding > tabblad Basisinstellingen > IP-adresinstellingen**.
3. Stel de gewenste netwerkparameters in.
4. Sla uw wijzigingen op.

DHCP inschakelen op apparaathardware

Afhankelijk van de mogelijkheden van het apparaat kan het IP-adres als volgt worden omgeschakeld:

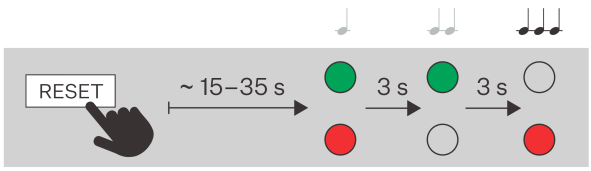
- met de RESET knop

TIP
Raadpleeg de installatiehandleiding van het product voor de locatie van de RESET-knop.

Een dynamisch IP-adres instellen met de RESET-knop

Volg de onderstaande stappen om de netwerkconfiguratie van het apparaat met een dynamisch IP-adres (DCHP ON) in te stellen:

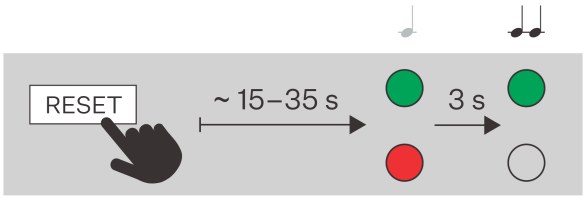
1. Houd de RESET-knop ingedrukt.
   a. Wacht tot de rode en groene LEDs op het apparaat gelijktijdig oplichten en het geluidsalarm afgaat (ongeveer 15-35 seconden).
   b. Wacht totdat de rode LED uitgaat en het geluidssignaal klinkt (ongeveer nog 3 seconden).
   c. Wacht tot de groene LED uit gaat en de rode LED weer gaat branden en u een geluidssignaal hoort dat aangeeft dat de batterij bijna leeg is (nog ongeveer 3 seconden).
2. Laat de RESET-knop los.



Een statisch IP-adres instellen met de RESET-knop

Volg de onderstaande stappen om de netwerkconfiguratie van het apparaat in te stellen op een statisch IP-adres (DHCP UIT):

1. Houd de RESET-knop ingedrukt.
   a. Wacht tot de rode en groene LEDs op het apparaat gelijktijdig oplichten en het geluidsalarm afgaat (ongeveer 15-35 seconden).
   b. Wacht totdat de rode LED uitgaat en het geluidssignaal klinkt (ongeveer nog 3 seconden).
2. Laat de RESET-knop los.



OPMERKING

Na het opnieuw opstarten zal het apparaat de volgende netwerkparameters hebben:

- IP-adres: 192.168.1.100
- Netmasker: 255.255.255.0
- Standaardgateway: 192.168.1.1

Toegang tot webgebaseerde apparaatconfiguratie

Het apparaat wordt geconfigureerd via een webgebaseerde configuratie-interface die toegankelijk is via een webbrowser.

Om toegang te krijgen tot de interface, moet u het IP-adres van het apparaat of de domeinnaam van het apparaat kennen. Het apparaat moet verbonden zijn met het lokale IP-netwerk en moet van stroom worden voorzien.

De webgebaseerde configuratie-interface is ook toegankelijk via het aangesloten My2N-portaal of via de configuratietool 2N Access Commander.

Inloggen op de webconfiguratie-interface

1. Start uw internetbrowser.
2. Voer het IP-adres van het apparaat of de domeinnaam van het apparaat in (zie hoofdstuk Apparaten op het netwerk vinden (p. 3)).
3. Als u geen certificaat hebt gegenereerd voor het IP-adres, kunt u een waarschuwing krijgen over een ongeldig beveiligingscertificaat. In dit geval moet u bevestigen dat u naar de webconfiguratie-interface wilt gaan.
4. Het aanmeldingsscherm wordt weergegeven.

5. Voer uw inloggegevens in.
   De standaardreferenties zijn:
   - Gebruikersnaam: **Admin**
   - Wachtwoord: **2n**
6. Wijzig uw wachtwoord na de eerste keer inloggen.

Toegang vanaf 2N Access Commander

1. Meld u aan bij de interface Access Commander.
2. Ga naar Apparaten.
3. Druk voor het geselecteerde apparaat op .

Wachtwoord wijzigen

U moet het standaardwachtwoord wijzigen om volledige toegang te krijgen tot de functies van de webconfiguratie-interface. U kunt het apparaat niet configureren zonder het standaard wachtwoord te wijzigen.

TIP

Het wordt aanbevolen om een wachtwoord te gebruiken dat moeilijk te kraken is. Het wordt afgeraden om namen, plaatsnamen of namen van voorwerpen in wachtwoorden te gebruiken, met name als deze een directe link hebben met de gebruiker.

Voor een hogere wachtwoordbeveiliging raden wij aan:

- gebruik maken van een willekeurige wachtwoordgenerator
- een wachtwoordlengte van minimaal 12 tekens
- een combinatie van verschillende tekens uit verschillende tekensets (bijvoorbeeld kleine/hoofdletters, cijfers, speciale tekens, enzovoort)

Aanbevolen browsers

De webconfiguratie-interface is geoptimaliseerd voor Chrome-gebaseerde webbrowsers (zoals Google Chrome, Microsoft Edge of Opera). Als u andere browsers gebruikt, kunnen er kleine verschillen in functionaliteit zijn in het uiterlijk van de interface.

Basisinstellingen apparaat

Firmware-update

Nieuwe firmwareversies zijn beschikbaar op de updateserver. Als de webconfiguratie-interface geen toegang heeft tot het openbare internet, is het mogelijk om het firmwarebestand handmatig naar het apparaat te uploaden.

OPMERKING
Firmware-updates worden niet automatisch uitgevoerd. Om de integriteit van het systeem te waarborgen en onbedoelde fouten te voorkomen, moeten alle updates handmatig door de gebruiker worden bevestigd of gestart. Controleer voordat u een update uitvoert de release notes voor de nieuwe versie en controleer de compatibiliteit met uw bestaande infrastructuur.

De firmware ophalen van de updateserver

1. Ga naar **Systeem > Onderhoud > tabblad Firmware**.
2. Klik op Controleren op updates.
3. Wanneer er een update beschikbaar is, worden de release notes geladen. Om de upgrade te starten, klikt u op Upgrade in de koptekst van het venster.
4. Nadat de firmware met succes is geüpload, wordt het apparaat automatisch opnieuw opgestart. Na het herstarten is het apparaat volledig beschikbaar met de nieuwe firmware. Firmware-updates hebben geen invloed op de configuratie.

Nieuwe firmware uploaden vanuit opslag

1. Ga naar **Systeem > Onderhoud > tabblad Firmware**.
2. Klik op Firmware uploaden.
3. Selecteer in het dialoogvenster dat wordt geopend een bestand uit uw eigen archief.
4. Bevestig het uploaden van het bestand door te klikken op Upload.
   Het apparaat controleert het firmwarebestand en zal niet toestaan dat een onjuist of beschadigd bestand wordt geüpload.
5. Nadat de firmware met succes is geüpload, wordt het apparaat automatisch opnieuw opgestart. Na het herstarten is het apparaat volledig beschikbaar met de nieuwe firmware. Firmware-updates hebben geen invloed op de configuratie.

OPMERKING
De functionaliteit, betrouwbaarheid en veiligheid van het apparaat hangen af van de geïnstalleerde firmware. Het regelmatig bijwerken van de firmware naar de huidige versie maakt deel uit van de gebruiksvoorwaarden van het product. Fouten die veroorzaakt kunnen worden door het gebruik van een verouderde firmwareversie kunnen niet geclaimd worden. De huidige firmware implementeert klantervaringen en vereisten op het gebied van de beveiliging van persoonlijke gegevens.

Directory

De sectie Directory is een belangrijk onderdeel van de apparaatconfiguratie. U maakt gebruikers aan in de directory en beheert hun toegangsrechten.

Handmatig een gebruiker aan een map toevoegen

1. Klik op de pagina Directory op Gebruiker toevoegen.
2. De gebruikersgegevens worden geopend. Geef de gebruiker een naam op het tabblad Persoonlijke gegevens.
3. Stel de toegangsopties in volgens Benaderingen (p. 10).

Bulkbeheer van gebruikers in Access Commander of My2N

Als het apparaat wordt beheerd via Access Commander of My2N-hulpprogramma's voor bulkconfiguratie, worden alle wijzigingen in de webgebaseerde configuratie-interface overschreven door de instellingen in het hulpprogramma voor bulkconfiguratie. Een gebruiker die rechtstreeks in de webinterface is aangemaakt, wordt verwijderd.

In de kolom holder in de directorytabel staat het bulkconfiguratietool waarmee de gebruiker is aangemaakt. De kolom houder is standaard verborgen.

Benaderingen

Een van de basisfuncties van het apparaat is het beheren van de toegang en het ontgrendelen van het elektrische deurslot. Het apparaat beheert de toegang op basis van de evaluatie van toegangsverzoeken volgens vooraf gedefinieerde toegangsregels. Als het apparaat het verzoek als legitiem beoordeelt, activeert het de deurschakelaar die het elektrische deurslot bedient. Hierdoor wordt de deur ontgrendeld.

Naast conventionele gebruikersauthenticatie (RFID-kaart, biometrie, Bluetooth, enz.) kan de schakelaar ook worden geactiveerd met behulp van externe signalen en interfaces, waardoor flexibele integratie- en automatiseringsopties mogelijk zijn. De verschillende manieren om de deurschakelaar te activeren worden hieronder beschreven:

Verificatie van gebruikers

De gebruiker gebruikt zijn authenticatiemethode en als zijn gebruikersrechten in overeenstemming zijn met de toegangsregels, wordt hem toegang verleend. Toegestane toegang activeert de deurschakelaar.

De instelling wordt beschreven in het hoofdstuk Instellingen voor gebruikerstoegang (p. 12).

Schakelaarbediening in de webconfiguratie-interface

1. Ga naar **Integratie > Schakelaars**.
2. Zoek de schakelkaart die de deur bedient.

> **OPMERKING**
> De functie van de deurschakelaar in het apparaat wordt uitgevoerd door **Schakelaar 1**.

3. Klik onder **Handmatige schakelaarbediening** op Houd ingedrukt.
4. De schakelaar blijft aan totdat u de handmatige bediening weer annuleert.

Uitschakelen op basis van tijdprofiel

In de webconfiguratie-interface kunt u de schakelaar zo instellen dat de deur gedurende een vooraf bepaalde tijd ontgrendeld blijft, bijvoorbeeld tijdens de lunchpauze.

1. Ga naar **Integratie > Schakelaars**.

2. Zoek de schakelkaart die de deur bedient.

> **OPMERKING**
> De functie van de deurschakelaar in het apparaat wordt uitgevoerd door **Schakelaar 1**.

3. Klik op de pijl → van de geselecteerde schakelaar om naar de details te gaan.
4. Schakel op het tabblad **Status** de optie **Tijdgestuurde hold-schakelaar** in.
5. Selecteer de tijdsprofielen waarin de schakelaar moet worden vastgehouden of voer een aangepaste tijdsperiode in.

Uitschakelen van een oproep (DTMF)

DTMF-code-instellingen

1. Ga naar **Integratie > Schakelaars**.
2. Zoek de schakelkaart die de deur bedient.

> **OPMERKING**
> De functie van de deurschakelaar in het apparaat wordt uitgevoerd door **Schakelaar 1**.

3. Klik op de pijl → van de geselecteerde schakelaar om naar de details te gaan.
4. Op het tabblad **Activeringscodes van**, kunt u de codes instellen die u via DTMF kunt invoeren tijdens een gesprek met het apparaat.
   De geldigheid van elke code kan beperkt zijn in de tijd.

> **OPMERKING**
> Voor de eerste activeringscode kunt u instellen dat deze als een oudere vorm van de code wordt verwerkt. In deze vorm hoeft u de code niet met een sterretje te bevestigen wanneer u deze op het toetsenbord van de telefoon invoert.

De DTMF-code gebruiken

1. Wanneer u met het apparaat verbonden bent, voert u de activeringscode in op het toetsenbord van uw telefoon en bevestigt u met een sterretje.

> **OPMERKING**
> Het ontvangen van DTMF-signalen is standaard ingeschakeld op het apparaat. U kunt de machtigingen controleren op de pagina Gespreksservice (SIP/Lokale gesprekken) onder het tabblad **Audio**, op het tabblad **DTMF ontvangen**.

Verbinding verbreken met HTTP API

Het volledige gebruik, inclusief een beschrijving van de benodigde HTTP API autorisatie, wordt beschreven in de HTTP API handleiding voor 2N apparaten. De deurschakelaar wordt bestuurd door het eindpunt `api switch ctrl`. Voor schakelaar 1 ziet het commando er als volgt uit: `https://ip_adresa/api/switch/ctrl?switch=1&action=on`.

Uitschakelen door automatisering

De configuratie van de automatisering wordt beschreven in de handleiding Automation. De schakelaar wordt geactiveerd door de actie **ActivateSwitch**.

Instellingen voor gebruikerstoegang

Om zich met succes te authenticeren bij de toegangscontrole-eenheid en de deur te ontgrendelen, moet de gebruiker aan twee voorwaarden voldoen: toegangsrechten hebben toegewezen aan het apparaat en ten minste één authenticatiemethode hebben ingesteld. De beschikbare verificatiemethoden hangen af van het specifieke apparaat en kunnen RFID-kaarten, numerieke PIN-codes, QR-codes voor scannen met de camera, enz. zijn.

Authenticatie-instellingen:

1. Ga naar **Directory**.
2. Open de gebruikersdetails door op de rij te klikken of selecteer Gebruiker toevoegen om een nieuwe gebruiker aan te maken.
3. Op het tabblad **Authenticatie** stelt u alle methoden in waarmee de gebruiker zich zal authenticeren, zie Authenticatiemethoden (p. 12).
4. Vul op het tabblad **Access Settings (Toegangsinstellingen) van** in wanneer de gebruiker toegang moet krijgen om naar binnen en naar buiten te gaan.
   - Wanneer dan ook
   - Tijdsprofiel - biedt ingestelde **Tijdsprofielen**
   - Aangepast - gebruik de knop Bewerken om tijdsintervallen in te stellen die uniek zijn voor deze gebruiker.

   Stel een vervaldatum in om de toegang van de gebruiker tot een bepaalde kalenderperiode te beperken.
   Door **Uitzonderingen** toe te kennen, krijgt de gebruiker permanente toegang die zelfs de tijdelijke vergrendeling van het door de toegangsregels aangegeven apparaat niet beperkt (zie Toegangsregels (p. 14)).

Authenticatiemethoden

LET OP
De beschikbare verificatiemethoden zijn afhankelijk van het specifieke apparaat en de aangesloten modules.

RFID-kaart

Aan één gebruiker kunnen maximaal 2 RFID-kaarten worden toegewezen.

De identificatie kan handmatig worden ingevoerd met het toetsenbord of worden gelezen door de kaart in een USB-lezer te steken die op de computer is aangesloten.

Vereisten voor RFID-kaarten

- De identifier moet een hexadecimaal getal zijn.
- De minimale lengte van de identifier is 6 tekens.
- Alleen kaarten die door het apparaat worden ondersteund, kunnen worden gebruikt - het kaarttype moet ingeschakeld zijn in de module-instellingen (zie **Access > Modules**).

TIP
U kunt de identificatie van een bestaande kaart uit het log lezen op **System > Event Log**. Laad de nieuwe/niet-toegewezen kaart op het apparaat en kopieer vervolgens de identificatie (UUID) ervan uit het logboek. Nadat het identificatiemiddel tussen de RFID-kaarten is geplaatst, kan de gebruiker de kaart gaan gebruiken voor verificatie.

My2N
My2N – gebruikt om verbinding te maken met de applicatie My2N authenticatie via Bluetooth inschakelen.

PIN-code / QR-code
De PIN-code dient als een persoonlijke numerieke toegangscode, die de gebruiker invoert op het toetsenbord van het apparaat of kan worden gelezen door de camera van het apparaat in de vorm van een QR-code.

LET OP
QR-codes kunnen alleen worden gelezen met de interne camera van het apparaat.

PIN-vereisten

- De minimale lengte is 2 cijfers.
- De code kan alleen cijfers (0-9) bevatten.
- QR-codes kunnen alleen gebruikt worden voor PIN-codes die tussen de 4 en 15 cijfers lang zijn.
- Als u de functie **Stil alarm** gebruikt, raden wij u aan even genummerde PIN-codes aan te maken.

OPMERKING
Wanneer u een hexadecimale QR code gebruikt, moet de waarde omgezet worden naar decimaal formaat voordat u deze invoert.

Geaccepteerd hexadecimaal bereik: 1000 tot FFFFFFFF.

Vingerafdruk
Elke gebruiker kan tot 2 vingerafdrukken uploaden. Gebruik een externe vingerafdruklezer om ze te uploaden. Controleer of u het 2N USB-stuurprogramma hebt geïnstalleerd. Het stuurprogramma kan hier worden gedownload https://www.2n.com/en-GB/download-center/?type=driver .

De geüploade vingerafdruk van een gebruiker kan voor de volgende acties worden gebruikt:

- Open de deur;
- Een stil alarm starten - kan alleen worden ingesteld als de functie Deur openen actief is;
- Automation F1 en F2: genereert de FingerEntered-gebeurtenis in Automation. F1 en F2 worden gebruikt om de aangesloten vinger in Automatisering te onderscheiden.

Kenteken

Sommige apparaten ondersteunen nummerplaatherkenning met behulp van externe AXIS-camera's die zijn uitgerust met de add-on toepassing **VaxALPR**. Herkende nummerplaten worden in een HTTP-verzoek naar het eindpunt `api/lpr/licenseplate` gestuurd (meer HTTP API-handleiding voor IP-intercoms).

TIP
De procedure voor het toevoegen van een externe camera wordt beschreven in ???.

Nummerplaat – stelt de kentekenplaat van het voertuig van de gebruiker in, die het apparaat kan scannen en gebruiken om de gebruiker te authenticeren.

Vereiste nummerplaat:

- De maximale lengte van een nummerplaat is 10 tekens.
- Er kunnen maximaal 20 nummerplaten aan één gebruiker worden toegewezen.
- Elke kentekenplaat mag slechts aan één gebruiker worden toegewezen - als er meerdere toewijzingen zijn, wordt de eerst gevonden record gebruikt.
- De nummerplaten worden gebruikt in de herkenningsfunctie van het externe camerabeeld (zie Interoperabiliteitshandleiding).

Virtuele kaart

De virtuele kaart wordt gebruikt om de gebruiker te identificeren in apparaten die via de Wiegand interface zijn aangesloten. Na succesvolle authenticatie van de gebruiker via de My2N-toepassing of op de biometrische lezer, wordt de virtuele kaart-ID naar de Wiegand interface verzonden (als het verzenden van identifiers is ingeschakeld in de configuratie, zie **Toegang > Toegangsregels > Tabblad Toegang/Uitgang > Geavanceerd**).

Vereisten voor virtuele kaart:

- De ID moet een hexadecimaal getal zijn (tekens 0-9, A-F).
- De ID kan 6 tot 32 tekens lang zijn.
- Een gebruiker kan slechts één virtuele kaart toegewezen krijgen.

Schakelcode

Schakelcode – maakt het instellen van maximaal 4 codes mogelijk voor het activeren van schakelaars (bijv. deurslot). Om het slot te openen met het toetsenbord op het apparaat wordt naast de schakelcode ook een DTMF-code gebruikt.

Toegangsregels

De pagina **Toegang > Toegangsregels** stelt de parameters en logica in voor het ontgrendelen van de deur, die wordt beheerd door de deurschakelaar van het apparaat. Deze configuratie bepaalt hoe toegangsverzoeken (authenticatie) worden geëvalueerd, de voorwaarden die nodig zijn voor succesvolle gebruikersautorisatie en de regels voor het beheer van individuele toegangen.

Terwijl u individuele machtigingen definieert in de gebruikersinstellingen, bepalen toegangsregels wanneer, onder welke voorwaarden en hoe deze machtigingen kunnen worden gebruikt. U kunt bijvoorbeeld instellen of deurdoorgang slechts in één richting is toegestaan, of authenticatie een stil alarm kan activeren, of dat de gebruiker zich slechts één keer per gedefinieerd tijdsinterval kan authenticeren.

Toestand van deur en slot

Op het tabblad Status kunt u zien of de deurschakelaar actief is en of de deur open is.

Deur

- “Open” - toegang is verleend, de deurschakelaar is gesloten en de deur kan worden geopend.
- “Gesloten” - de deur is vergrendeld en kan niet worden geopend.

Slot

- “Ontgrendeld” - de schakelaar is actief en kan worden bediend.
- “Vergrendeld” - de schakelaar is uitgeschakeld en kan niet door toegangsregels worden gecontroleerd.

TIP
De knop met het slotsymbool op dit tabblad wordt gebruikt om de schakelaar te vergrendelen of ontgrendelen vanuit de webinterface.

Deurdetectie

In het tabblad **Doors kan** ingeschakeld worden, zodat het ongeoorloofd openen van een deur of het langdurig openen ervan een gebeurtenis activeert. Deze gebeurtenis kan dan worden opgevolgd door automatiseringen. Gebeurtenissen worden ook naar het logo van het apparaat geschreven.

Aankomst en vertrek

Eén apparaat kan worden gebruikt om doorgangen in twee richtingen te beheren. U kunt enkele modules aan het apparaat aan de andere kant van de deur bevestigen en deze twee kanten dan afzonderlijk instellen. Zo kunt u beperken welk tijdstip van de dag doorgang wordt toegestaan in de richting **Arrival** en welk tijdstip van de dag doorgang wordt toegestaan in de richting **Departure**, of welke authenticatiemethoden worden geaccepteerd in een bepaalde richting, enz.

Module-indeling voor aankomst of vertrek

1. Ga naar **Toegang > Toegangsregels**.
2. Op het tabblad **Aankomst** of **Vertrek** onder **Modules** klikt u op Beheren.
3. Er wordt een dialoogvenster geopend met een lijst van beschikbare toegangsbeheermodules.
4. Sleep de modules in groepen volgens de richting die ze moeten geven.

TIP
Klik op om een specifieke module te zoeken. De module activeert een visueel of akoestisch signaal, afhankelijk van de mogelijkheden.

Toegangsregels

Toegangsregels bepalen welke authenticatiemethoden worden geaccepteerd om toegang te verlenen. Er kunnen meerdere toegangsregels worden ingesteld voor verschillende tijdsprofielen. Toegangsregels kunnen ook gebruikt worden om te bepalen wanneer toegang geweigerd moet worden.

U kunt toegangsregels gebruiken om de geaccepteerde verificatiemethoden te beperken, u kunt gebruikers bijvoorbeeld dwingen om van 8:00 tot 9:00 uur een RFID-kaart te gebruiken.

TIP
De authenticatiebeperking is handig om te gebruiken op een apparaat dat sleutels beheert voor **2N IP Fortis**. Gebruikers zullen dus genoodzaakt zijn om de sleutels voor **2N IP Fortis** op hun RFID-kaart regelmatig bij te werken.

Bij het instellen van de regels kunt u kiezen of u een zonecode wilt gebruiken om de deur te openen. **De zonecode** wordt toegepast wanneer het apparaat een zone krijgt in een bulkapparaatbeheer (zoals Access Commander). **De zonecode** kan ook handmatig worden ingesteld in het gedeelte **Geavanceerd**. Het werkt op dezelfde manier als **Schakelaar Activeringscode**; als u deze code op het toetsenpaneel van de module invoert, wordt de deurschakelaar geactiveerd.

Stiltewaarschuwing

Het stille alarm is een speciale manier om het slot te openen waarmee u onopvallend een beveiligingsactie in gang kunt zetten. Het stille alarm wordt vooral gebruikt in panden en gebouwen die in trek zijn bij overvallers - casino's, financiële centra, banken, enz. Na het invoeren van de PIN-code gaat de deur open, maar tegelijkertijd wordt het alarm geactiveerd zonder dat de aanvaller dit merkt.

Als u het stille alarm activeert, wordt de gebeurtenis **SilentAlarm** geactiveerd. Deze gebeurtenis kan bijvoorbeeld gevolgd worden door automatisering:

- Een HTTP-verzoek naar het beveiligingssysteem sturen.
- Foto's maken met de camera van het apparaat.
- Een oproep naar een vooraf ingestelde bestemming instellen.

Het stille alarm activeren

1. De gebruiker voert een code in die één hoger is dan zijn normale PIN-code.
   Voorbeeld: De gebruiker heeft een PIN-code ingesteld “1926”. Voer de code “1927” in om de deur te openen. De deur gaat open en het SilentAlarm-event wordt tegelijkertijd geactiveerd.

LET OP
Om de deur met een PIN-code te kunnen openen (zelfs als het Stil Alarm tegelijkertijd afgaat), is het nodig om het tabblad **In/Out onder** in te schakelen.

Toegang blokkeren na mislukte pogingen

Na vijf opeenvolgende mislukte toegangspogingen wordt de toegang gedurende 30 seconden geblokkeerd. Toegang zal gedurende deze periode niet worden toegestaan, zelfs als de gebruikersauthenticatie geldig is.

Deze functie blokkeert de toegang alleen door autorisatie van de gebruiker. De deurschakelaar kan ook door andere methoden worden geschakeld, zoals DTMF, HTTP-commando, enz.

QR-codes lezen

De aan de gebruiker toegewezen pincode voor toegang of de activeringscode van de schakelaar kan door de camera worden gelezen in de vorm van een QR-code.

Voor goed laden moet u **QR code leesmodus** instellen. De codes worden altijd in decimaal formaat in het apparaat opgeslagen. Bij het lezen in decimale modus moeten de gelezen QR-codes exact overeenkomen met de PIN-codes (4 tot 15 cijfers lang) die in het apparaat zijn opgeslagen. In hexadecimale modus worden QR codes na het lezen omgezet naar decimale getalnotatie en vervolgens vergeleken met de opgeslagen decimale codes. Vooraf toegewezen nullen worden genegeerd tijdens het hexadecimaal lezen.

OPMERKING
Geaccepteerd hexadecimaal bereik: 1000 tot FFFFFFFF.

Voor het lezen van QR codes kunt u het ook zo instellen dat alleen de gebeurtenis **CodeEntered** wordt geactiveerd in plaats van de deurschakelaar te bedienen. Deze gebeurtenis kan dan opgevolgd worden met verdere acties via Automations.

De gescande QR-code kan worden doorgestuurd naar een extern toegangscontrolesysteem dat communiceert via een Wiegand interface (zie ???).

Anti-passback

Anti-passback is een uitbreiding van het toegangscontrolesysteem die het opnieuw betreden gedurende een ingesteld tijdsinterval voorkomt. In deze modus zal het apparaat de gebruiker slechts één keer binnen een bepaalde tijd toestaan om in te voeren. Nadat een gebruiker met succes het systeem is binnengegaan, registreert het systeem deze gebeurtenis en kan de gebruiker pas weer toegang krijgen tot het systeem nadat de opgegeven tijd is verstreken. Deze tijd wordt ingesteld wanneer Anti-passback is ingeschakeld.

Anti-passbackmodi:

- “Hard” - De gebruiker kan gedurende de ingestelde tijd het apparaat in geen enkele richting passeren. De gebruiker krijgt geen toegang totdat het interval verloopt of de toegang wordt hersteld door de apparaatbeheerder.
- “Soft” - Regelovertredingen worden alleen gelogd en kunnen de beheerder waarschuwen, maar de gebruiker krijgt wel toegang.

Gegevensoverdracht voor Wiegand

LET OP
Om Wiegand-gegevens door te sturen, moet een Wiegand-uitbreidingsmodule correct op het apparaat zijn aangesloten. De Wiegand uitbreidingsmodule wordt meestal niet meegeleverd in de productverpakking.

Met de Wiegand doorstuurfunctie kan het apparaat de identificatiegegevens van de geverifieerde gebruiker doorsturen naar een extern toegangscontrolesysteem dat communiceert via de Wiegand interface. Dit garandeert de integratie van 2N-apparaten met traditionele toegangscontrolesystemen. Met deze instelling kunt u de juiste groep selecteren voor het routeren van gegevens.

Het doorsturen van data voor Wiegand wordt ingesteld in **Toegang > Toegangsregels > I/O > Geavanceerd**. Het versturen van autorisaties naar gebruikers die hun QR code gelezen hebben, wordt ingesteld in het tabblad **Access/Exit** voor het inschakelen van QR code lezen.

De deurschakelaar instellen

De deurschakelaar is een logische functie van het apparaat dat het elektrische deurslot bedient. De schakelaar kan op verschillende manieren geactiveerd worden (bijv. door HTTP-commando, RFID-kaart of DTMF-signaal).

De functie van de deurschakelaar in het apparaat wordt uitgevoerd door **Schakelaar 1**.

De pagina **Access > Modules** kan vervolgens worden gebruikt om een specifieke toegangsmodule toe te wijzen aan een andere schakelaar.

De deurschakelaar instellen

1. Sluit de elektrische contacten van het deurslot (bijv. magneetcontact) aan op de daarvoor bestemde ingang van de intercom.
2. Ga in de webconfiguratie-interface naar **Integration > Switches**.
3. Open de instellingen van schakelaar 1 door op de pijl in de tabkop te klikken.
4. Stel op het tabblad **Configuratie van de** schakelaar de parameters in van de hardware-uitgang die de deurschakelaar moet aansturen.
   - **Geregelde uitgang** - specificeert de uitgang die het elektrische deurslot schakelt.
   - **Modus** - Monostabiel / Bistabiel.
   - **Inschakeltijd** - stelt de inschakeltijd in monostabiele modus in. In de bistabiele schakelmodus is de ingestelde schakeltijd niet van toepassing.
   - **Uitgangstype** - in de modus “Security” werkt de uitgang in omgekeerde modus, wat betekent dat hij permanent ingeschakeld is en het beveiligingsrelais aanstuurt met een specifieke pulsvolgorde. Als u een omgekeerd deurslot gebruikt (d.w.z. het slot wordt vergrendeld wanneer er stroom op wordt gezet), stelt u het uitgangstype in op “Inverse”.

     TIP
     Als u een beveiligingsrelais gebruikt, stelt u het uitgangstype in op “Beveiliging”.

     Als er meerdere schakelaars met een verschillend ingesteld uitgangstype op één uitgang zijn aangesloten, worden ze aangestuurd volgens de volgende prioriteit:

     1. Security
     2. Invers
     3. Normaal
5. In de tabbladen **Activering** en **Activeringscodes** kunt u extra manieren instellen om de schakelaar te activeren. Als u geen andere methoden instelt, wordt de schakelaar alleen geactiveerd door gebruikerstoegang toe te staan.
6. Sla de wijzigingen op.

Modules

De pagina **Access > Modules** biedt centraal beheer van alle toegangshardwaretechnologieën op het apparaat. Elke module heeft een eigen tabblad op de pagina waarmee deze beheerd kan worden. Zowel modules die rechtstreeks in de hoofdeenheid van het apparaat zijn geïntegreerd als modules die via VBUS zijn aangesloten, worden hier beheerd.

Elke module kan een naam krijgen en een specifieke schakelaar toegewezen krijgen om te bedienen. Andere parameters zijn afhankelijk van het type module.

In de fabrieksinstellingen besturen alle modules de deurschakelaar.

OPMERKING
Als de firmwareversies van de aan te sluiten module en de hoofdeenheid niet compatibel zijn, wordt de module niet gedetecteerd. In dit geval moet u de firmware van het apparaat bijwerken (Firmware-update (p. 9)) nadat u de module hebt aangesloten.

Bluetooth-toegang instellen

Gebruikersauthenticatie via Bluetooth gebeurt via My2N-applicatie, die de gebruiker op zijn mobiele telefoon moet hebben gedownload.

GET IT ON Google Play Download on the App Store

LET OP
Het instellen van de koppelingscode moet momenteel in de oude configuratie-interface gebeuren.

Maak een koppelingscode op het apparaat

1. Ga naar **Directory** en open de gegevens van de gebruiker voor wie u de overeenkomende code wilt maken.
2. Klik in de kop van de webconfiguratie-interface op Ga naar de oude interface.
   Opent de gebruikersdetails in de oude configuratie-interface.
3. Klik in het blok **WaveKey** op .
   In het dialoogvenster dat wordt geopend, wordt een koppelingscode gegenereerd die u moet invoeren in de toepassing My2N op uw apparaat.
4. Open de My2N app en voer de koppelings-PIN in.

   OPMERKING
   Als u al een app met een ander apparaat hebt verbonden, kunt u de pincode voor koppeling invoeren via het pictogram Toevoegen boven aan het scherm.
5. Volg de instructies op uw mobiele telefoon - benader het apparaat in de koppelmodus en klik op Koppeling starten.

WAARSCHUWING
Voor mobiele telefoons met oudere besturingssystemen (Android 9 / iOS 17 en lager) moet u een applicatie gebruiken om te koppelen Mobile Key.

Koppelen in de mobiele app Mobile Key

1. Download de app Mobile Key naar uw mobiele telefoon. De applicatie is beschikbaar op App Store En Google Play.
2. Open de app en schakel de app in Mobile Key toegang tot Bluetooth.
3. Afhankelijk van het type mobiele sleutel, benadert u de USB-lezer of het koppelapparaat met de mobiele telefoon.
4. In de app Mobile Key klik op het aangeboden apparaat om te koppelen.
5. De applicatie vraagt u om een pincode in te voeren. Voer de koppelingscode in en bevestig de invoer ervan.

Bluetooth-verificatiemethoden

In de webconfiguratie-interface kunnen verschillende Bluetooth-verificatiemethoden worden ingesteld.

- **Direct in de mobiele app** - de gebruiker selecteert de deur die hij wil openen direct in de My2N mobiele app. Als zijn mobiele apparaat zich binnen het bereik van het 2N-apparaat bevindt, maakt het verbinding met het apparaat en als aan de toegangsregels wordt voldaan, wordt de deur ontgrendeld.
- **Door de mobiele telefoon dicht bij het apparaat te brengen en het apparaat aan te raken** - een gebruiker met een mobiel apparaat en Bluetooth ingeschakeld nadert het 2N-apparaat en raakt de Bluetooth-verificatieplaats op het 2N-apparaat aan, die meestal is gemarkeerd met het Bluetooth-pictogram . Zodra de verbinding tot stand is gebracht en de toegangsrechten zijn geverifieerd, wordt de deur ontgrendeld.
- **Bewegingsdetectie** - 2N apparaten met een camera detecteren beweging in de omgeving en activeren automatisch Bluetooth. Als een 2N-apparaat een mobiel apparaat van een gebruiker met geldige toegang binnen bereik detecteert, wordt de deur ontgrendeld.

Geaccepteerde Bluetooth-verificatiemethoden instellen

1. Ga naar **Toegang > Modules**.
2. Selecteer op het tabblad **voor de Bluetooth-module** de mogelijke methoden in het veld **Start Authentication**.
3. Als u “bewegingsdetectie” hebt geselecteerd, selecteer dan het profiel waarmee beweging moet worden gedetecteerd.

OPMERKING
Bewegingsdetectieprofielen worden ingesteld in **Aanpassing > Camera > Interne camera**.

Liftbesturing

Door de AXIS A9188 relaismodule aan te sluiten op een 2N intercom of op een 2N toegangscontrole-eenheid, kan de toegang tot afzonderlijke liftverdiepingen in het gebouw worden geregeld. Er kunnen maximaal 8 van deze relaismodules worden aangesloten op één intercom 2N of toegangseenheid 2N. Elk van de modules kan 8 verdiepingen besturen, dus in totaal maximaal 64 verdiepingen. Om deze functie te kunnen gebruiken, moet u een actieve licentie hebben: voor IP-intercoms (bestelnr. 9137916) of voor toegangseenheden (bestelnr. 9160401).

Liftaansluiting

1. Sluit de ingangen van de liftbesturingen aan op het AXIS A9188 relais en verbind het relais met het IP-netwerk. Noteer het IP-adres van het relais.
   Volg de documentatie voor de AXIS A9188 I/O-relaismodule, beschikbaar op http://www.axis.com.
2. Open de webconfiguratie-interface van het 2N-apparaat dat de lifttoegangen moet beheren.
3. Ga naar **Integratie > Toegangscontrole > Tabblad Lift**.
4. Op het tabblad **Relay Modules (AXIS A9188)** schakelt u een van de modules in.
5. Klik op het potloodpictogram en voer het IP-adres van de relaismodule in het geopende vak in.
6. Als de toegang tot het relais onderworpen is aan verificatie, voert u de gebruikersnaam en het wachtwoord in op het tabblad **Algemeen**.
7. Wanneer de relaismodule ingeschakeld is, verschijnen de verdiepingen die deze module beheert op het tabblad **Elevator Floors**. U kunt elke verdieping een naam geven.

Openbare toegang tot de vloer instellen

1. Selecteer op het tabblad **Elevator Floors (liften)** de verdiepingen die toegankelijk moeten zijn voor het publiek (toegang is niet afhankelijk van autorisatie).

2. Klik op het potloodpictogram naast de geselecteerde verdieping.
3. Schakel in de geopende instellingen **Publieke toegang in.**
4. Beperk optioneel de toegangstijd voor het publiek door een tijdsprofiel te selecteren of een aangepaste toegangstijd in te stellen.

Geavanceerde instellingen

Camera- en video-instellingen

De camera van de **2N Access Unit QR** detecteert beweging rond het apparaat en leest QR-codes.

Interne camera-instellingen

1. Ga naar **Aanpassing > Camera**.
2. Op het tabblad **Interne camera** klikt u op →.
3. Op het tabblad **Instellingen** kunt u de basis beeldparameters van de camera bewerken.
4. Na het opslaan worden de wijzigingen weergegeven in het voorbeeld van de camera.

Modus

Met de cameramodus kunt u de optimale combinatie van belichtingsmodus en stroomfrequentie instellen om stabiele beelden van hoge kwaliteit te verkrijgen. Deze modus wordt gebruikt om ongewenst flikkeren te verminderen dat kan optreden bij gebruik van kunstlicht of wanneer de netfrequentie varieert. Bij installatie van camera's binnenshuis kan een geschikte methode voor het onderdrukken van flikkering door lichtbronnen worden geselecteerd, terwijl bij plaatsing buitenshuis een onderdrukkingsmodus voor direct zonlicht kan worden geactiveerd om een optimale beeldaanpassing aan de huidige lichtomstandigheden te garanderen.

IR LED

De IR LED-achtergrondverlichtingsfunctie wordt gebruikt om een beeld van hoge kwaliteit te garanderen, zelfs bij weinig omgevingslicht. Deze modus wordt geactiveerd wanneer de lichtomstandigheden onder het ingestelde niveau komen. Het grensniveau van de lichtomstandigheden wordt pas ingesteld nadat de IR LED-verlichting is ingeschakeld.

OPMERKING
Als het toegestane stroomverbruik overschreden zou kunnen worden - bijvoorbeeld wanneer meerdere uitbreidingsmodules met PoE-voeding tegelijkertijd in werking zijn - wordt het IR-vermogensniveau automatisch geoptimaliseerd om de stabiliteit van het apparaat te handhaven.

Geavanceerde instellingen

Dag-/nachtmodus - hiermee kunt u schakelen tussen afbeeldingen in kleur en afbeeldingen in zwart-wit, afhankelijk van de lichtomstandigheden. Stel **Always Day** in als u wilt dat de camera een IR-onderdrukkingsfilter gebruikt en de IR-achtergrondverlichting uit is. De instelling "Always Night" daarentegen schakelt het filter uit en de IR-verlichting in, waardoor het beeld overschakelt naar de zwart-witmodus, geschikt voor nachtzicht. De automatische modus schakelt de camera tussen deze twee toestanden op basis van het omgevingslichtniveau.

Lokaal contrast - verbetert details en texturen door de helderheidsverschillen tussen aangrenzende gebieden van de afbeelding (randen) te vergroten.

Tone Mapping - verhoogt de helderheid en zichtbaarheid van de afbeelding, maar kan lichte kleurvervorming veroorzaken.

Maximale belichtingstijd - Specificeert de maximale tijd dat de afbeelding wordt belicht. Wanneer er meer licht beschikbaar is, is het mogelijk dat de sluiter niet de hele tijd open is en zal de camera automatisch een kortere belichtingstijd instellen.

Bewegingsdetectie

Bewegingsdetectie op 2N-apparaten is een functie die automatisch beweging detecteert in het gezichtsveld van de interne camera en waarmee u verschillende acties kunt activeren, zoals het activeren van Bluetooth of het verzenden van een melding.

Voor optimale prestaties kan de detectie gekalibreerd worden aan de omgeving en omstandigheden, bijvoorbeeld door de gevoeligheidsparameters en het gebied dat door de camera bewaakt moet worden te wijzigen.

Instellingen bewegingsdetectie

1. Ga naar **Aanpassing > Camera**.
2. Op het tabblad **Interne camera** klikt u op .
3. Op het tabblad **Camera Preview** klikt u op het potloodpictogram naast de parameter **Motion Detection**.
4. Er wordt een venster geopend met de profielinstellingen voor bewegingsdetectie.
5. Vouw het tabblad uit van het profiel dat u wilt instellen.
6. Door het vierkant in het cameravoorbeeld aan te passen van een specifiek gebied waarin de camera beweging moet opnemen.

> **LET OP**
> Het afbeeldingsgebied is relatief ten opzichte van de huidige afbeeldingsuitsnede. Als u de uitsnede van het camerabeeld wijzigt, zullen de bestaande gebieden hetzelfde blijven, maar effectief een ander deel van de ruimte bedekken. Het is daarom altijd aan te raden om deze gebieden te controleren en aan te passen na het bewerken van een uitsnede.

7. Selecteer de motion capture-modus voor het profiel, zie Profielmodi (p. 23)
8. Pas indien nodig andere parameters aan volgens de modus.
9. Vergeet niet om het profiel altijd in te schakelen!
10. Om uw wijzigingen op te slaan, klikt u op de knop **Opslaan** of **Opslaan en sluiten** bovenaan de pagina.

Profielmodi

Gebeurtenissen triggeren

In deze modus legt de camera ogenblikkelijke, eenmalige bewegingen vast. Een voorbeeldgebruiksgeval is het maken van een foto wanneer iemand een kamer binnenkomt of wanneer een voertuig in de buurt van het apparaat passeert.

De activering van de getriggerde gebeurtenis kan worden vertraagd met behulp van de ingestelde vertraging.

Gebruik het filter om de soorten bewegingen te definiëren die u door de camera wilt laten negeren - bijvoorbeeld kleine objecten (kleine vogels) of herhalende bewegingen (bomen in de wind).

Bezig met uploaden

Dit profiel activeert een gebeurtenis van 30 seconden wanneer beweging wordt gedetecteerd. Als er gedurende deze tijd een andere beweging plaatsvindt, zal het profiel alles in één gebeurtenis combineren. Deze modus is geschikt voor continue bewaking en voorkomt het aanmaken van een groot aantal korte records.

Gebruik het filter om de soorten bewegingen te definiëren die u door de camera wilt laten negeren - bijvoorbeeld kleine objecten (kleine vogels) of herhalende bewegingen (bomen in de wind).

Gezichtsdetectie
Het profiel detecteert beweging wanneer een gezicht in het bewaakte gebied verschijnt. Een gebeurtenis kan ook plaatsvinden wanneer een statische afbeelding van een gezicht (bijv. een foto) in het frame verschijnt.

Detectie van binnenkomende personen
Het profiel herkent alleen bewegende mensen en negeert statische afbeeldingen van gezichten.

Privacybeleid
De privacyfunctie maskeert een deel van het beeld zodat het niet zichtbaar is of opgenomen wordt in de video. Deze optie is ideaal voor situaties waarin u bijvoorbeeld gevoelige delen van de afbeelding wilt beschermen. Als het apparaat bijvoorbeeld bij de receptie wordt geplaatst en de camera ook de gang vastlegt waar vreemden zich bewegen, kunt u de gang verbergen.

LET OP
Privacybescherming kan de activiteit van het lezen van QR-codes of bewegingsdetectie beperken. We raden niet aan om tegelijkertijd privacybescherming en deze functies te gebruiken.

Instellingen bewegingsdetectie

1. Ga naar **Aanpassing > Camera**.
2. Op het tabblad **Interne camera** klikt u op .
3. Op het tabblad **Camera Preview** klikt u op het potloodpictogram naast de parameter **Privacy**.
4. Pas in het voorbeeld van de camera het vierkant aan om het gebied dat u wilt maskeren te bedekken.

   LET OP
   Het afbeeldingsgebied is relatief ten opzichte van de huidige afbeeldingsuitsnede. Als u de uitsnede van het camerabeeld wijzigt, zullen de bestaande gebieden hetzelfde blijven, maar effectief een ander deel van de ruimte bedekken. Het is daarom altijd aan te raden om deze gebieden te controleren en aan te passen na het bewerken van een uitsnede.

5. Selecteer de cloakingmodus:
   - **Kleur** - het geselecteerde gebied wordt bedekt met de kleur van uw keuze
   - **Mozaïek** - het geselecteerde gebied wordt gepixeld. Stel de grootte van het mozaïek in volgens het vereiste niveau van gegevensanonimisering.
6. Vergeet niet om privacybescherming in te schakelen in de koptekst van de parameterinstellingen!
7. Om uw wijzigingen op te slaan, klikt u op de knop **Opslaan** of **Opslaan en sluiten** bovenaan de pagina.

Externe camera
De externe camera wordt als videostream (RTSP) aan het 2N-apparaat toegevoegd. Door een externe camera aan te sluiten, kunt u tijdens een gesprek schakelen tussen weergaven. De functie van de externe camera is dus puur beeldvorming.

LET OP
QR-codes kunnen alleen worden gelezen met de interne camera van het apparaat.

Een externe camera toevoegen

1. Ga naar **Aanpassing > Camera**.
2. Selecteer onder het tabblad **Externe camera** Camera toevoegen.
3. In het dialoogvenster dat wordt geopend, schakelt u de camera in.
4. Voer het stream-bronadres van de externe IP-camera in, in het formaat `rtsp://ip_address_camera/parameters`.
5. Als de externe camerastream moet worden geauthenticeerd, vult u **in met de inloggegevens voor de stream**.
6. Sla uw wijzigingen op door te klikken op Camera toevoegen.
7. Als de externe camera de hoofdcamera van het apparaat moet worden, klik dan na het opslaan op het tabblad **External Camera** op Set as default source.
   Wanneer u met het apparaat praat, wordt eerst het beeld van de camera weergegeven die als standaardbron is ingesteld.

Een videostream van de apparaatcamera maken

De IP videostreamingfunctie wordt gebruikt om live video van de camera van det apparaat via het netwerk naar een ontvangend apparaat te sturen, zoals een app op een mobiele telefoon, volgsoftware of op een computer in een videospeler. Dit proces zorgt ervoor dat gebruikers vanaf verschillende apparaten real-time video kunnen bekijken.

Een videostream maken

1. Ga naar **Integratie > Video**.
2. Activeer de **RTSP server service**.
3. Stel de stream-parameters in, zie Video stream-parameters (p. 25).
4. Op het tabblad **Connection Restrictions (Verbindingsbeperkingen)** kunt u de IP-adressen invullen vanwaar de stream beschikbaar zal zijn. Als er geen IP-adressen zijn ingevuld, is het mogelijk om vanaf elk IP-adres verbinding te maken.
5. Geef op het tabblad **Voorgeconfigureerde streams** aan of de stream toegankelijk moet zijn:
   - anoniem
   - met verificatie - stel de verificatiegegevens in op het tabblad **Verificatie**.
6. Op het tabblad **Voorgeconfigureerde streams** vindt u de IP-adressen van de geconfigureerde streams volgens de geselecteerde video codec.

Video stream-parameters

Algemene stream-instellingen

Jittercompensatie - stelt de lengte van de buffer in om ongelijke intervallen tussen aankomsten van audiopakketten te compenseren. Een langer geheugen betekent een hogere weerstand tegen uitval, maar meer audiovertraging.

QoS DSCP waarde - stelt de prioriteit in van audio en video RTP pakketten in het netwerk. De ingestelde waarde wordt verzonden in het TOS (Type of Service) veld in de IP-pakketheader.

Enable UDP unicast mode - schakelt de modus in voor het verzenden van audio- en videostreamgegevens met behulp van het RTP/UDP-protocol. Als deze modus is uitgeschakeld, worden audio- en videostreamgegevens altijd alleen via het RTP/RTSP-protocol verzonden.

Initial RTP port - stelt de initiële lokale RTP-poort in het 60-poorts bereik in die gebruikt wordt voor audio- en videotransmissie. De standaardwaarde is 4800 (d.w.z. het gebruikte bereik is 4800-4859).

Zipstream - selecteert het standaard Zipstream compressieniveau (voor H.264). AXIS Zipstream bewaart alle belangrijke forensische details die u nodig hebt en vermindert de vereisten voor gegevensoverdracht en opslag met gemiddeld 50%.

Aangepaste formaatstromen instellen

1. Op het tabblad **Streams van het aangepaste formaat** klikt u op Genereer stream URL. Er wordt een dialoogvenster geopend.
2. Stel in het dialoogvenster in:
   - **Codec** - selecteert uit beschikbare codecs
   - **Audio inschakelen** - specificeert of alleen video of video met audio moet worden verzonden
   - **Resolutie** - stelt de resolutie van de afbeelding in
   - **Framerate** - stelt de framerate van de opgenomen video in
   - **Bitrate** - stelt de bitrate in
   - **Zipstream** - selecteert het standaard Zipstream compressieniveau (voor H.264). AXIS Zipstream bewaart alle belangrijke forensische details die u nodig hebt en vermindert de vereisten voor gegevensoverdracht en opslag met gemiddeld 50%.
3. Het streamadres met parameters wordt automatisch geladen onderaan het dialoogvenster.
4. Kopieer het streamadres en sla uw wijzigingen op.

Geluidsinstellingen

Het volume van het apparaat instellen

Om het volume van uw apparaat aan te passen, gaat u naar **Aanpassing > Audio**.

Gebruikersgeluiden

Het apparaat voert verschillende acties uit die gepaard gaan met geluid (rinkelen, schakelen, enz.). U kunt de geluiden die worden afgespeeld wijzigen in **Aanpassing > Gebruikersgeluiden**.

U kunt ook tot 10 aangepaste gebruikersgeluiden uploaden naar het apparaat.

Andere audiofuncties van het apparaat

Ruisdetectie

Het apparaat kan het door de microfoon ontvangen geluid controleren en wanneer het signaalniveau van de microfoon een ingestelde drempel overschrijdt, kan het apparaat een gebeurtenis `Event.NoiseDetected` oproepen. Deze gebeurtenis kan gevolgd worden door andere gebeurtenissen in de automatisering (zie Automatisering (p. 33)).

Activering van ruisdetectie

1. Ga naar **Integratie > Audio**.
2. Schakel de functie in de kop van het tabblad **Ruisdetectie** in.
3. Geef in de parameter **Ruisdrempelniveau** de waarde [dB] op die de gebeurtenis **Event.NoiseDetected** activeert wanneer deze wordt overschreden.
4. In de parameter **Alarm Start Delay** kunt u instellen hoe lang het geluid boven een drempelniveau moet zijn voordat de gebeurtenis wordt geactiveerd.
5. In de parameter **Alarm End Delay** kunt u daarentegen de tijd specificeren dat het signaal onder de drempel moet zijn om de gebeurtenis te beëindigen.

Audiotest

Het resultaat van de laatste test kunt u vinden op **Integratie > Audio > tabblad Algemeen > tabblad Audiotest**.

2N-apparaten kunnen de ingebouwde luidspreker en microfoon regelmatig controleren. Tijdens de test genereert de luidspreker in het apparaat een of meer korte tonen. Met behulp van de ingebouwde microfoon wordt de gegenereerde toon waargenomen en als deze correct wordt gedetecteerd, wordt de test geslaagd verklaard. De duur van de test is ongeveer 4 s. Als de test niet succesvol is (wat bijvoorbeeld veroorzaakt kan worden door extreem omgevingsgeluid), wordt de test na tien minuten nogmaals herhaald. Het resultaat

van de laatste test kan worden weergegeven in de webgebaseerde configuratie-interface van het apparaat of worden verwerkt met Automatisering.

OPMERKING
Als er een gesprek gaande is wanneer de audiotest wordt gestart, wordt de audiotest uitgesteld totdat het gesprek beëindigd is. De audiotest vindt direct na afloop van het gesprek plaats.

Tijdprofielen

Sommige functies die het apparaat uitvoert, zijn tijdsafhankelijk. Met de sectie **Tijdsprofielen van** kunt u vooraf tijdsintervallen instellen waaruit u vervolgens kunt kiezen voor deze functies. Dit betekent dat u de tijd niet telkens handmatig hoeft in te voeren. U kunt het tijdsprofiel een naam geven voor meer duidelijkheid.

Een tijdprofiel aanmaken:

1. Ga naar **Aanpassing > Tijdsprofielen**.
2. Klik op leeg om een nieuw profiel aan te maken.
3. Voer een profielnaam in.
4. Klik op Opslaan. De profielgegevens worden geopend.
5. Stel de intervallen in waarop het tijdsprofiel actief moet zijn.
   1. Klik op het gewenste interval.
   2. U kunt het begin en einde opgeven in het geopende menu.

   OPMERKING
   De regel **Vakantie** wordt gebruikt om verschillende tijdsintervallen in te stellen tijdens de geselecteerde dagen, zie Feestdagen (p. 27).
6. Sla de wijzigingen op.

Feestdagen

In de apparaatconfiguratie kunt u verschillende dagen definiëren die als vakantiedagen worden gemarkeerd. Voor deze dagen worden dan speciale intervallen ingesteld in de tijdsprofielen. Meestal zijn dit dagen zoals feestdagen, bedrijfsvakanties en andere speciale dagen.

Voor elke feestdag geeft u aan of deze alleen voor een bepaald jaar geldt of elk jaar op dezelfde dag herhaald wordt. Vakanties kunnen meerdere jaren van tevoren gepland worden.

Vakantie-instellingen:

1. Ga naar **Aanpassing > Tijdsprofielen > tabblad Vakantie**.
2. Selecteer het jaar waarvoor u de feestdag wilt instellen.
3. Klik op de dag in de kalender:
   - De eerste klik markeert de feestdag die elk jaar op de opgegeven dag en maand herhaald zal worden.
   - Een tweede klik verandert de vakantie in een eenmalige vakantie voor het geselecteerde jaar.
4. Sla de wijzigingen op.

De veiligheidsschakelaar instellen

De tamper-schakelaa detecteert het openen van het deksel van het apparaat, wat door de software wordt geëvalueerd als een logische sluiting van de schakelaar. Op deze manier geeft de schakelaar aan dat er mogelijk fysiek met het apparaat geknoeid is.

Wanneer u een tamper-schakelaa activeert, kunt u alle andere schakelaars uitschakelen of Automatisering instellen om een vervolgactie te activeren, zoals het verzenden van een e-mail, het aanmaken van een HTTP-verzoek of het activeren van een stil alarm.

OPMERKING
Afhankelijk van het type apparaat kan de beveiligingsschakelaar in de hoofdeenheid worden geïntegreerd of moet deze als extra module worden geïnstalleerd. Raadpleeg de installatie-handleiding van het specifieke apparaat voor meer informatie over de installatieprocedures.

Blokkeren van andere schakelaars wanneer het deksel geopend wordt

Het apparaat zorgt ervoor dat de andere schakelaars worden geblokkeerd tijdens het openen van de afdekking (d.w.z. wanneer de veiligheidsschakelaar wordt geactiveerd). Dit voorkomt ook dat de deurschakelaar wordt geactiveerd en voorkomt toegang via de deur die het apparaat bedient.

Instelprocedure voor schakelaarblokkering

1. Ga naar **Integratie > I/O**.
2. Wijs op het tabblad **Beveiligingsschakelaar** een beveiligingsschakelaar toe aan de ingang.
3. Schakel de optie **Automatische schakelblokkering in**.

Beveiligingsschakelaargebeurtenissen

Activering van de beveiligingsschakelaar activeert gebeurtenissen. Deze gebeurtenissen kunnen worden gekoppeld aan Automatisering (p. 33).

- Het openen van het deksel triggert de gebeurtenis `TamperSwitchActivated (status: in)`.
  Als de schakelaar als ingang wordt toegewezen in **de I/O-sectie**, wordt een extra gebeurtenis `Input-Change (poort: tamper, status: false)` gegenereerd.
- Het sluiten van het deksel activeert de gebeurtenis `TamperSwitchActivated (status: uit)`.
  Als de schakelaar is toegewezen als ingang **aan de I/O-sectie**, wordt een extra event `InputChange (poort: tamper, status: true)` gegenereerd.

Systeem

Datum- en tijdinstellingen

LET OP
Als het apparaat wordt beheerd door een massamanagementtool (2N Access Commander / 2N My2N), kan de apparaattijd door deze tool worden beheerd. Handmatige wijzigingen in de webinterface van het apparaat hebben geen invloed op de tijdsinstelling.

Synchronisatie met NTP

Als het apparaat op internet is aangesloten, kunnen de tijd en datum gesynchroniseerd worden met behulp van NTP.

1. Ga naar **Systeem > Datum en tijd**.
2. Op het tabblad **van Tijdsynchronisatie-instellingen** activeert u de optie **Automatische tijd van NTP of Internet**.
3. Voer het adres van de NTP-server van uw keuze in.

Tijdsupdate bij stroomuitval

1. Ga naar **Systeem > Datum en tijd**.
2. Op het tabblad **van Time Sync Settings** klikt u op Sync with Browser.
   Hierdoor wordt de tijd op het apparaat gesynchroniseerd met de tijd op uw computer.

OPMERKING
De 2N-apparaten zijn uitgerust met een real-time back-upklok waarmee u een stroomstoring tot meerdere dagen kunt overbruggen.

Netwerkinstellingen

Standaard gebruikt het apparaat een dynamisch IP-adres dat door de DHCP-server wordt toegewezen.

Een juiste IP-adresconfiguratie is essentieel om ervoor te zorgen dat uw apparaten op een stabiele en betrouwbare manier met uw netwerk verbonden zijn.

1. Om de netwerkparameters van het apparaat in te stellen, gaat u naar **Systeem > Netwerkverbinding**.

2. Onder Basisinstellingen > IP-adresinstellingen kunt u de DHCP-server in- of uitschakelen.

Instelling voor een statisch IP-adres:

a. Schakel de optie **DHCP server** uit.
b. Voer het gewenste IP-adres, subnetmasker, standaard gateway en DNS-servers in.
c. Sla uw wijzigingen op. Start het apparaat opnieuw op.

DHCP-instellingen

a. Schakel de optie **DHCP server** in.
b. Voer het gewenste IP-adres, netmasker, standaard gateway en DNS-servers in.
c. Sla uw wijzigingen op. Start het apparaat opnieuw op.

OPMERKING
Als u een RADIUS-server en een op 802.1x gebaseerd verificatiemechanisme gebruikt voor aangesloten apparaten in uw netwerk, kunt u het apparaat configureren om EAP-MD5- of EAP-TLS-verificatie te gebruiken. Het tabblad 802.1x wordt gebruikt om deze functie in te stellen.

Licenties

Sommige functies zijn alleen beschikbaar onder de juiste licentie. Voor een overzicht van licenties en of ze actief zijn, zie **Systeem > Licenties > tabblad Algemene informatie.** Op het tabblad **Licensed Features** vindt u een overzicht van de beschikbare functies waarvoor een licentie vereist is.

OPMERKING
Neem na het selecteren van de juiste licentie contact op met uw 2N-dealer. Als u een 2N partner bent, kunt u contact opnemen met onze klantenservice op customercare@2n.com. Vermeld het serienummer van het apparaat in uw verzoek.

De licentiesleutel bijwerken

De huidige licentiesleutel is beschikbaar op de updateserver. Als de webconfiguratie-interface geen toegang heeft tot het openbare internet, kunt u het sleutelbestand handmatig uploaden naar het apparaat.

Telkens wanneer het apparaat opnieuw wordt opgestart, wordt de laatst beschikbare licentiesleutel opnieuw geladen.

Proeflicentie

Met de proeflicentie kunt u tijdelijk alle functies van de Gold-licentie en Microsoft Teams-licentie gebruiken gedurende maximaal 800 uur na activering. Een geactiveerde proeflicentie kan niet worden opgeschort.

Om een proeflicentie te activeren, gaat u naar **Systeem > Licenties > tabblad Proeflicentie**.

LET OP
Telkens wanneer het apparaat opnieuw wordt opgestart, wordt een uur van de proeflicentie verwijderd.

Gebruikte poorten

Dienst	Poort	Protocol	Richting	Standaard ingeschakeld	Verstelbaar	Instellingen
802.1x	–	–	In/Out	×	×	–
DHCP	68	UDP	In/Out	✓	×	–
DNS	53	TCP/UDP	In/Out	✓	×	–
Echo (device discovery)*	8002	UDP	In/Out	✓	×	–
FTP	21	TCP	Out	×	×	–
2N IP Eye	8003	UDP	Out	×	×	–
HTTP	80	TCP	In/Out	✓	✓	**Systeem > Netwerkverbinding > tabblad WEB-SERVER**
HTTPS	443	TCP	In/Out	✓	✓	**Systeem > Netwerkverbinding > tabblad WEB-SERVER**
NTP-client	123	UDP	In/Out	✓	×	–
SLP	427	UDP	In/Out	✓	×	–
SMTP	25	TCP	Out	×	✓	**Integratie > Kennisgeving per e-mail**
Syslog	514	UDP	Out	×	×	–

Dienst	Poort	Protocol	Richting	Standaard ingeschakeld	Verstelbaar	Instellingen
TFTP	69	UDP	Out	×	×	–
My2N Knocker	443	TCP	Out	✓	×	–
My2N Tribble Tunnel	443	TCP	Out	✓	×	–
SNMP Agent	161	UDP	In/Out	✓	×	–
SNMP Trap	162	UDP	Out	✓	×	–
Multicast receiver (Automation)	4433	UDP	In	×	×	–
Multicast DNS	5353	UDP	In/Out	✓	×	–

Automatisering

De standaard 2N apparaatconfiguratie is geschikt voor de meest voorkomende scenario's. Voor geavanceerde gevallen, zoals de noodzaak om het apparaat aan te passen aan specifieke vereisten of te integreren met systemen van derden, kan de automatiseringsfunctie worden gebruikt. Met automatisering kunt u aangepaste logica definiëren voor apparaatgedrag dat reageert op verschillende gebeurtenissen, signalen of combinaties van omstandigheden. Specifieke acties kunnen bijvoorbeeld worden geactiveerd door op een specifieke snelkiestoets te drukken, een stil alarm te activeren, een open deur te detecteren, een ingang te activeren of beweging in de buurt van het apparaat te detecteren.

Automatiseringsinstellingen:

1. Ga in de webinterface van het apparaat naar **Integration > Automation**.
2. Schakel in het functieoverzicht het gewenste aantal functies in.
3. Klik op  om de configuratie-interface van de automatisering te openen.
4. Typ in de kop van de interface Automations de naam van de functie waaronder de functie zal worden opgeslagen.
5. Maak een automatiseringsstroom.
   Een gedetailleerde beschrijving van de functie en configuratie van Automatisering is beschikbaar in de handleiding Automatisering van Automation.
6. Wanneer de functie voltooid is, klikt u op SAVE en verlaat u de automatiseringsinterface.

Toegangslezers – Configuratiehandleiding

2N.com